Please Support Independent Media | Make A Small Donation

The BritCard Psyop | True Digital ID + Digital Twins

TRUTH11.COM

Oct 17, 2025 17 min

Iain Davis | substack.com/@iaindavis

The proposed rollout of the so-called BritCard is a bait-and-switch ps
operation (psyop). The evident purpose is to frame the debate about
UK by fundamentally misrepresenting what digital ID is.

Subscribe

People often say “if you don’t have anything to hide what’s the problem?” There is no rational argument for allowing people you don’t know and have never met to have any power to control your life. The “nothing to hide” mantra is based on the historically illiterate assumption that you will never have anything to fear from authority. To offer this argument as a reason to adopt digital ID is so naive we might call it stupid.

Of course, the likes of Trilateralist Starmer and Larry Ellison’s buddy Tony Blair will be delighted if we agree to a BritCard or a similar single, government issued identity app. But the whole point of arguing for and against the adoption of the mythical BritCard is to lead people to believe that if they reject the BritCard they will have defeated digital ID. And that is simply not true.

If you elect the next government because it promises not to introduce BritCard you will have done less than nothing to stop the rollout of digital ID in the UK, nor its imposition on you. It is already here. The digital prison walls have been built. Now the sole remaining task of our would-be gaolers is to entice us inside and lock the doors behind us.

BritCard is obviously a ruse. As Kit Knightly from the Off-Guardian rightly observed, if the BritCard smartphone app is “mandatory” then smartphones will also have to be “mandatory.” Do you really think successive UK governments would have invested so much in digital ID infrastructure only to risk the whole project pivoting on the take-up of a single smartphone app that the population can reject with ease? Of course not. So what is UK digital ID?

Most of us have been using UK digital ID practically every day for years. For example, both your driving license and your passport, if they were issued in the last decade, are digital ID products that have Machine Readable Zones (MDZs) embedded in them. MDZ’s can be scanned and the private data contained therein extracted by compliant systems and entered on to relevant databases where it can be searched, interrogated, cross referenced and manipulated.

In the case of the UK driving license, for instance, the photograph of you face is a biometric—biological identifiers—recorded and entered onto the various public and private databases via Identity Document Validation Technologies (IDVT). This is why

official photo requirements are so specific. Clause 95 of the proposed Crime and Policing Bill, which is progressing unhindered through the lobbies, could well see 55 million UK driver's faces entered onto the "biggest biometric database ever created in the UK." Rejecting BritCard won't stop this data seizure.

When you file a tax return online, have your face scanned at the automated tills or in an airport, and especially when your "verify" yourself online, or with a government or bank official, you are and have been constructing your "digital twin." This ongoing rollout of UK digital ID is a process undertaken by both the public and the private sectors.

By way of example, let's consider how Elon Musk's 'X' harvests your data to create your "digital twin." Musk's X is not alone in doing so, pretty much all social media companies use the same sort of systems and network of "verification partners."

Musk contracts with the Israeli company AU10TIX, which is a subsidiary of the Israeli intelligence-founded ICTS. AU10TIX explains how your UK digital ID functions:

> Digital ID functions as a Digital Twin of your identity. [. . .] Digital IDs continuously validate your identity using biometrics, [. . .] your Digital ID evolves with risk signals, fraud prevention insights, and changing credentials—ensuring it remains accurate and trustworthy. [. . .] A true Digital ID isn't just tied to one institution. It's reusable across banks, government services, airlines, and online platforms.

People who are not "verified" on X have not submitted their facial recognition image, unless they used it in their profile. Therefore, for those users, X has yet to harvest their facial recognition biometrics. This is why, since 2023, Musk wants X-users to "verify" themselves using their biometrics—facial recognition image. This ties your physical, *real* self to your digital twin. And there is a great deal that flows from that.

With all this infrastructure already in place, you might wonder why the government needs us to give it any more data or further permission to access it. Why not just use what it already has at its disposal?

The problem for the government and it partners is that all this data sits in "disparate data sets." It is spread out across different databases that use different formats and

structures. It hasn't been "fused" and is not a "coherent" single data set that can be used to fully control us, yet.

As noted by AU10TIX, as we use our digital ID products, the system evolves with us. The use of the products constantly updates our so-called "risk signals." How those risk signals are judged and by whom then becomes the question. Nevertheless, as the Israeli intelligence cut-out highlights, "true Digital ID" is used by "banks, government services, airlines, [. . .] online platforms," and more.

Therefore, to achieve "true Digital ID," the harvested data needs to be "interoperable." It has to be fused and become coherent so that AI can analyse, extract, manipulate and insert data into our digital twin as and when desired.

"True Digital ID" serves both the public and the private sectors. Both government and multinational corporations evaluate your "risk signals"—whatever they deem them to be—and treat you accordingly. Which, often, is not very well.

The UK digital ID products, that we all carry around and use today, represent components of the "true Digital ID" system. The system will bind together all of your licenses, contracts, permits and cards, all records of your interactions with online and offline services, all you health data, all payment platforms you use, every transaction you make, and all data from all other government and commercial services you use.

Your "true Digital ID" is constructed and develops systematically whenever you interact with the system, be it in a council office, a supermarket, a hospital or a bank. In fact, pretty much anywhere and everywhere.

The UK government is currently trying to fix your "true Digital ID" to *all* access points. Thus making your ability to interact with wider society conditional on the public-private partnerships'—the state's—systematic assessment of your individual "risk signals."

This system-wide, or "interoperable," digital ID network is what the UK government is actually trying to coerce us into adopting. Though the government would be cock-a-hoop if we accepted the BritCard gateway into the system, BritCard has virtually nothing to do with it.

When Labour Together—the dodgy Labour think tank that bunged Starmer into the Labour leadership—first concocted its BritCard PR stunt it made a couple of telling comments:

> For a progressive society to work, it needs to be able to collectively agree who is allowed to join it. Because it will exclude those who cannot join it.

Just to be clear: digital ID will permit or deny your access to society. If your "risk signals" aren't up to scratch you will be excluded. The Fabian's continued:

> [BritCard will build] on the existing One Login and Gov.UK Wallet. [. . .] All the necessary elements of the technology needed to deliver BritCard exist and are already in use in multiple arenas.

This is partially true. Certainly, all the necessary elements of UK digital ID, including One Login and GOV.UK Wallet, already exist and are commonly in use, but they are not "needed to deliver BritCard." They are *needed* to subject us all to the rigours of "true Digital ID" interoperability and, thereby, limit our behaviour to whatever is permitted by the public-private state.

Though One Login is *conveniently* available as a smartphone app, you can also "register your details" by other means. You could "answer security questions online" or prove you exist at a UK Post Office using your existing biometric digital ID products like your passport, driving license, or UK biometric residence card, for example.

Probably, many people who wish to resist digital ID in the UK—imagining it to be the BritCard—will choose one of the alternative options, such as registering using a third party Authorised Corporate Service Provider (ACSP). Unfortunately, that means the ASCP or the Post Office will still enter your details into the system for you and you will still be subjected to "true Digital ID." Though initially, you might wrongly assume you won't.

One Login is a single sign-on (SSO) service which authenticates the users online access to government, or rather GOV.UK "services." Currently, your One Login SSO only controls your access to forty-seven essential services, without which, if you need them, your life will be put on hold.

Things like signing a mortgage deed, applying for a vehicle operators license, canceling a lost of stolen passport, driving with a medical condition, applying for a grant, etc. Obviously, this doesn't give the government enough digital control over your life, so thankfully it promises that "access [to] all services on GOV.UK" will be "mandatory" and through One Login soon, by which they mean December 2027.

One Login is overseen by Government Digital Service (GDS), part of the Department for Science, Innovation and Technology (DSIT). "Think Digital Partners," (TDP) recently convened its "Cybersecurity and Digital Identity for Government" event with its partners including GDS, the Home Office, the Department of Defence, the Department of Work and Pensions, Microsoft, Amazon, and PricewaterhouseCoopers (PWC), etc.

TDP tells us:

> By the end of 2027, digital identity system One Login will become the only way to access all central government services.

Speaking at the TDP soiree, Natalie Jones, director for digital identity at GDS, said:

> Citizens don't experience their lives in terms of government departments. They experience them in terms of getting jobs, starting families, buying homes or planning retirement. One Login is helping us organise around those real-world needs.

Natalie Jones: director for digital identity at the Government Digital Service (GDS)

When Jones refers to "us" organising *all* citizens' "real-world needs," she means GDS and their partners. Sure, in order to get a job, start a family, buy a home or plan our retirement, we do sometimes have to deal with the government and its private sector partners. So, One Login will probably seem *convenient* for millions.

Apparently, eleven million of us have already signed up for UK "true Digital ID." If the governments plans proceed, these people won't be able to do any of those things "legally" without their digital ID. So they better hope their "risk signals" don't go off-track for any unforeseeable reason.

With regard to the alternative verification options—via an ASCP or the Post Office for instance—that people opposed to the BritCard might choose, Jones refers to them as "inclusion routes" and added:

> They're essential components of a digital identity system that serves all citizens.

One of the many drawbacks with the GOV.UK's One Login digital ID plan is that it is extremely high risk for "us"—meaning "us." Though it is outstanding at harvesting every scrap of data about our lives, there is no reason at all to imagine it is secure. Part of

the problem is that millions of people will access and use One Login and not all of them will be entirely honest.

In May this year, the *Telegraph* reported that One Login whistleblowers noted:

> [T]he One Login project [developers] had been routinely accessing the system without the required security clearance and background checks on laptops that were not secure. Some development on One Login was even taking place in Romania, without the top leadership's knowledge. Foreign intelligence services are active in Romania, which is a favourite with cyber criminals. All of this should have alarmed senior management at GDS, but instead, their response was to disband the whistleblower's team.

This cycbersecurity debacle resulted in One Login losing its Digital Identity Attributes Trust Framework (DIATF) accreditation only a few months ago. It still hasn't regained it but it's totally fine for everyone to use this hopelessly insecure life-or-death system now. Or so says the government, absent any plausible explanation.

When a gang of Bulgarian fraudsters committed £54 million benefit heist between 2016 and 2021, they used UK government online services to do it. Specifically, they targeted the online Universal Credit application service which moved into the even weaker cybersecurity realm of One Login in 2023. Far from protecting public safety, "true Digital ID" will usher us into the technological equivalent of the mythical Wild West.

To be fair, rubbish One Login cybersecurity is to be expected because SSO systems are inherently vulnerable. As noted by business-to-business technology specialists T*echTarget*:

> An attacker who gains control over a user's SSO credentials will be granted access to every application the user has rights to, increasing the amount of potential damage.

GDS is very unlikely to admit its treasured One Login has been compromised. If, by the end of 2027, One Login is "the only way to access all central government services,"

then being hacked seems likely and potentially devastating.

Good luck trying to convince GDS—and the police—that you did not fraudulently apply for benefits or a government grant. With access to your digital ID facial recognition data and the national public-private network of digital surveillance cameras, there will be no escape. Your "risk signals" will be awful. "The computer says no" could well have very grim consequences.

So let's say millions more of us hurl ourselves into the abyss and, for some inexplicable reason, volunteer to live under this evident public-private tyranny: where will all the seized data go and who will have access to it?

The generated data sets will be held by the GDS' GOV.UK. If we look at the GOV.UK so-called privacy notice, we note the first private sector corporation to get hold of your data is the multinational data broker Experian.

On behalf of the government, Experian will scrutinize and record your "true Digital ID" in order to *verify* your identity. It can do this easily enough by checking "your UK current account details against the details held by banks across the UK." So, right off the bat, through Experian, your "government" digital Identity service—One Login—suddenly involves your private sector bank account.

Most of us in the UK have been forced to use Experian's credit check service at some point in our lives. Of course, Experian isn't overly secure either, having been hacked by "identity thieves" a number of times. But don't worry, just "trust" the government and its partners. What could go wrong for you and your family?

A big part of Experian's business empire is based on selling data internationally. So having a contract with the UK government to hoover up the data from every citizen is fantastic news for Experian's leading investment shareholders, represented by, as usual, BlackRock and Vanguard.

Pausing a moment: we need to understand that the GOV.UK considers us its customers. In turn, Experian sees GOV.UK as one of its customers. Furthermore, in Public-private legalese jargon "we may" or "we might" means "we reserve the right" or, more succinctly, "we will."

This is important when we consider Experian statements like this:

> The information you provide to Experian Consumer Services might be used by Experian Marketing Services to: validate and update IP address, postal address and age details; create models into the 'make-up' of the UK population for characteristics across age, gender, number of adults and composition of the household and length of residency; identify when you change address; in linking profiled data about you to a client's customer file (where you are already their customer).

This means Experian will use your IP address, your physical address, all your personal details, including your family's details, and your financial data to track you and provide *profiles* about you to their customer, GOV.UK, because you are "already" a GOV.UK customer.

And:

> We will use automated systems to collect information from [your] bank and credit card accounts, which includes transactions for the last 12 months (incoming, outgoing, including payments) and account balance and other information, such as (account name, number, sort code, fees, charges, interest, benefits and rewards) in order to conduct analysis. [. . .] We may use your information for the investigation, detection and prevention of crime (other than fraud).

Experian *will* use your data for financial "investigations" that won't have anything to do with fraud. The commitment to the *prevention* of crime also means that you can be investigated by GOV.UK's partner—Experian and others—regardless of your standing as a *good citizen* and whether or not they actively suspect you of a crime. It's all about *safety* and *prevention* you see.

And:

> Your data may also be shared with other lenders or brokers as part of services we have developed to help them understand customer behaviours. [. . .] Where possible, this information will be provided in an anonymised or pseudonymised way.

Note: “where possible” means “we don’t have to, and we probably won’t.”

Sharing your data with any corporate partners, for any reason, is all part of the “true Digital ID” system in the UK. As GOV.UK points out:

> The data we collect may be shared with other government departments, agencies and organisations. It *may* also be shared with our technology suppliers.

GOV.UK data *will* be shared with every branch of government, including the intelligence agencies, and it *will* be shared with the government’s technology suppliers. This includes every corporation, like Deloitte, Mastercard, that have DIATF accreditation.

Other “technology suppliers” include Palantir and it is through their partnership with the UK government that we can really start getting to grips with the immense threat that “true Digital ID” presents to all of us in the UK.

Here’s a reasonable summary of Palantir’s relationship with the UK government:

> Palantir [. . .] has established a significant and growing footprint within the United Kingdom. The company primarily offers its sophisticated data integration, analytics, and AI-powered decision-making platforms, such as Palantir Foundry and Gotham, to help complex organizations manage and interpret vast datasets. Its involvement spans critical public and, increasingly, private sectors within the UK.

Palantir Gotham can scrape data from “any” source, such as satellite data, social media chatter, government digital ID data and any data set held by any government department or agency or private sector “customer” or partner. Palantir Gotham is capable of “data fusion.” This means it can translate data, no matter what the source or

format, into a single, coherent and actionable data set. It is primarily used by governments.

Palantir Foundry has commercial applications and is more widely used by the private sector. Like Gotham, Foundry "fuses" data sets to enable AI to interrogate the disparate data sources to produce meaningful outcomes and reports.

Palantir Gotham and Foundry are underpinned by Palantir Apollo software. This means Palantir can push data and software updates to any system connected to either Foundry or Gotham.

The UK government already uses and is connected to both Gotham and Foundry.

The government explains that Gotham and Foundry "integrates siloed data," i.e., "fuses" it from any source. It enables investigations and analysis "across all data." And it does mean "all."

The use of Apollo, inherent in both Gotham and Foundry, means that system wide "new functionality" can be introduced at any time.

This, then, is the essence of "true Digital ID" in the UK:

Your data, entered via One Login, is not safe and it is not secure. The government and an expanding list of private sector partners "will" have access to that data. The data will create your ultimate "digital twin" and that will be linked to your real, physical self via your harvested biometrics.

Every transaction you make, every comment you utter on social media, every political rally you attend, every donation you make, everywhere you go, and everything you do can and will be analysed, interrogated and manipulated. If your "risk signal" is awry you *will* be cut off. So you better behave as required.

All the government needs us to do is somehow dupe us into submitting our data to One Login. Hence, the BritCard bait-and-switch.

Once we step over the One Login Rubicon, our biometrics and all our data can be linked to our *official* "digital twin." Thereafter, the entire interoperable system can be centrally managed—almost certainly by AI—to "allow" or "exclude" us from society in order to control us.

In the immediate term, the only way to stop digital ID slavery is not to comply and refuse to create our One Login accounts. This will make life harder, we will be cut off, but it essentially boils down to what part of your soul you are willing to trade for the sake of permissioned convenience.

(Check out Fiona Rose Diamond's Mass Non Compliance for further information.)

In the longer term, I suspect the law is the arena where this battle will be won or lost. For us, this is a battle for our survival as free human beings. I'm no expert on the law, but the government's gambit to insist that we "must" have digital ID to live and work in the UK may be "legal" but it doesn't appear to be lawful. And lawful trumps legal every time.

The 1688 Bill of Rights compels the government never to undertake any "Proceedings to the Prejudice of the People." Threatening the people with the loss of their livelihoods and their rights and customs if they don't submit to digital ID is, it seems to me, to the prejudice of the people. But what do I know?

As we approach the point of no return perhaps we might ask the government why it needs to force people who don't want anything to do with its digital ID system to use it. If it is just for our convenience and safety, and not about social control, then what's the problem with us maintaining paper-based administrative services for the likely minority who don't want digital ID?

You could even imagine volunteers or small businesses providing this paper only service to the non-digital market. We might even reinvigorate the postal service. If "true Digital ID" is not about enforcement and control, and if we are willing to take on the responsibility ourselves, what possible objections could the government raise?

Image: Source [Edited]

Original Article: https://iaindavis.substack.com/p/the-britcard-psyop-what-is-true-digital

Related:

The BritCard Digital ID Psyop | A Bait and Switch

OffGuardian.org | Kit Knightly Iain Davis | IainDavis.com Apparently, in order to be able to work in the UK, we will all be forced to adopt digit...

Truth11.com

AlongID | Global Digital ID

Global Digital ID Has Been Tested and Will Be Showcased to Policymakers Next Week SHTFPlan.com | Mac Slavo Rhoda Wilson | T...

Truth11.com

Totalitarianism | Digital ID and Digital Currencies in Europe and the UK

John Gideon Hartnett | BibleScienceForum.com Now Europe and the UK are really pushing digital ID and digital currencies. It's not for their...

Truth11.com

Digital ID = Technocratic Control

DavidIcke.com | Neil Hauge Mike Fairclough You can already hear it, can't you? The dreary chorus of 'nothing to hide, nothing to fear.' Soo...

Truth11.com

Digital ID = Government Prison

HenryMakow.com Leon Hill Australia just passed its Digital Identity Bill into law.I'm Australian, but live in Iceland: a country that already has a...

Truth11.com

COMMENTS (0)

Subscribe to Truth11.com

Receive Articles By Email • Support Independent Media

Subscribe now

Support Truth11.com | • Make A Donation

• Become A Monthly Subscriber

TRUTH11.COM | Armed With The Truth • United We Stand

© Truth11.com 2025